Testimony

Statement for the Record

Martin Casado, Senior Vice President

Networking and Security Business Unit

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Science, Space, and Technology

Cyber Security: What the Federal Government Can Learn from the Private Sector

January 8, 2016

Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and Members of the Committee, thank you for the opportunity to testify today. I am Martin Casado, Senior Vice President and General Manager of Networking and Security at VMware. I have a PhD in computer science from Stanford University and began my career at Lawrence Livermore National Laboratory where I worked on network security in the Information Operations Assurance Center (IOAC).

My employer, VMware, is the fourth largest software company in the world, with 2014 revenues of over $6 billion and over 18,000 employees. VMware has more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. VMware serves all sectors of the U.S. Federal Government, the Civilian agencies, the Department of Defense, and the Intelligence Community as well as state and local governments. The company is headquartered in Silicon Valley, and given the Committee's leadership; I'd like to acknowledge we have a significant presence in Virginia and Georgia along with approximately 140 other offices throughout the world.

VMware is a leading provider of software-defined solutions that make data centers across the globe operate more efficiently and securely and allow both government and commercial organizations to respond to dynamic business needs. In 2012, it acquired the company I co-founded, Nicira, which greatly expanded VMware's capabilities in cyber security. Today, VMware is providing enhanced security to commercial and government customers globally through its pioneering role in redefining how we build and secure networks and data centers.

Cyber-Attacks: Clear and Persistent Threat to the U.S. Government

The U.S. Government is dependent on a vast cyber world of interconnected IT networks, data centers, the Cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission critical function within their purview, from national defense and natural disaster response to postal services and the constitutionally mandated Census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber-systems

has reaped immeasurable benefits for the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern day functions of Government, sophisticated and aggressive cyber-attacks perpetuated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. Well-publicized cyber-attacks have targeted the U.S. Postal Service, the U.S. Department of Commerce, the U.S. State Department, the Internal Revenue Service, and other agencies. In one of the largest cyber-attacks on a U.S. agency, and the reason for this important joint hearing, the Office of Personnel Management (OPM) suffered what appears to be one of the most damaging breaches of information ever on government workers. As you know, the OPM breach has potentially compromised the personal data and security of over 21 million current and former federal employees and has likely compromised our national security, national defense, and national intelligence posture(s). This breach has put our nation's blood and treasure at risk.

The recent attacks on our Government and within the private sector have had one thing in common: the attacker, once inside the network perimeter security, was able to move freely around the victim's network.

Given the recent string of cyber-attacks on our government, it is not a surprise that our collective trust in our cyber infrastructure, on which agencies are so dependent, is at risk. Without doubt, we are currently engaged in an escalating cyber arms race with entities that are methodical, sophisticated, and effective. They will continue to probe our cyber infrastructure for vulnerabilities and they will continue to exploit our agency's networks whenever possible.

It is clear to our nation and to those who perpetuate these attacks that the way in which we protect our national cyber infrastructure, the way in which we design and deploy cyber security systems across federal agencies, is insufficient.

As is apparent from publicized accounts, the nature of the security breach at OPM is not particularly unique. Hackers were able to penetrate perimeter network security systems and subsequently gain access to OPM and Department of Interior systems, where they were free to access and steal sensitive data over a period of several months. Hackers typically use this attack

methodology because traditional perimeter-centric security systems are structurally designed to be "doors" to the network. These systems allow authorized users access to networked systems and prevent unauthorized users from entering a network or data center. However, perimeter security is a single point of entry (a single perimeter: firewall + additional security systems like intrusion prevention or advanced attack detection) that must be breached or circumvented in order to enter the data center network. Once the intruder has passed the perimeter security there is no simple means to stop malicious activity from propogating throughout the data center. In many cases, the response from agencies and network security vendors is to add more security technology to the perimeter, which ignores the structural issue.

Mitigating the economic, political, and social damage to our nation from these types of cyber-attacks demands that we change the way we build, operate, and secure our Government's mission critical IT infrastructure.

VMware submits three salient points for consideration:

1) Every recent agency breach has had one thing in common: the attacker, once inside the perimeter security, has been able to move freely around the agency's network.
2) Perimeter-centric cyber security policies, mandates, and techniques are necessary, but insufficient and ineffective in protecting U.S. Government cyber assets alone.
3) These cyber-attacks will continue, but we can greatly increase our ability to mitigate them and limit the damage and severity of the attacks when they do.

Address the Threat: Immobilize the Attacker Inside the Network

In today's legacy networks, in government as well as the commercial sector, there are a lot of perimeter-centric technologies that are designed to stop an attacker from getting inside a network – clearly this approach is not sufficient to combat today's cyber-attacks. Perimeter-centric security solutions are analogous to a locked door that can only be accessed with a key. The primary function of the door is to deny initial unauthorized entry by anyone who does not have a key. However, once the door is forced open (hacked or breached), the unauthorized actor is free to move throughout (laterally) unabated.

In order to effectively prevent an Attacker from moving freely around the network, agencies must compartmentalize their existing network perimeter security by adding "Zero Trust" or "micro-segmented" network environments *within* the data center. A zero trust environment prevents unauthorized lateral movement within the data center by establishing automated governance rules that manage the movement of users and data between business systems and/or applications within the data center network. When a user or system "breaks the rules," the potential threat incident is compartmentalized and security staff can take any appropriate remediation actions. To build on the analogy above, compartmentalization is equivalent to securing each interior room with locks. Only those with the full key ring can move freely within the data center. Limiting the intruder's ability to move around freely within the house significantly mitigates the magnitude of a perimeter security breach, or break-in.

Address the Threat: Raise the Standard for Cyber Security

Cyber attacks pose a real and imminent threat to U.S. national security. Every agency needs to develop a sense of urgency and needs to be incentivized to do something beyond the status quo, because the current approach it is not working. We know the threat landscape is constantly evolving; as soon as one vulnerability is mitigated, another threat vector arises. The attackers deploy software that is being written, updated, and refined on a daily basis and this fact puts our agencies at a tactical disadvantage on a daily basis. Put simply, agencies that rely on a hardware-based perimeter security strategy cannot keep pace in a dynamically changing software-defined world.

Clearly, our nation's security posture needs to be significantly upgraded inside the network perimeter and throughout the data center. New cyber security approaches, such as Zero Trust and micro segmentation, should be adopted to enhance the government's cyber security practices. These new approaches are already the gold standard for commercial industry and need to become the gold standard across the Federal Government. VMware has implemented architectures leveraging these approaches in industries that are technology early adopters such as banking and universities. To facilitate this adoption in the federal government, policies such as FISMA should establish ratio metrics for the number of systems or workloads that a given system can access before passing though a security control. Typical agency networks have a

ratio of 1 to hundreds or 1 to thousands. The target ratio should be 1 to ones or 1 to tens so that if a given network is breached, the damage will be significantly constrained. Metrics will enable Government mandates and policies (e.g. FISMA) to withstand today's cyber warfare reality.

While there is no silver bullet to permanently address every cyber security threat, Congress can mandate that agencies adopt policies and security standards that mitigate threats inside the network perimeter.

Address the Threat: Secure Existing Cyber Infrastructure

VMware supports almost every federal agency in the U.S. Government in some part of their data centers. We have seen many agencies conclude that the most effective means of mitigating the potential for a breach is to build a new network environment or data center (a "greenfield" environment) with enhanced security protocols and new perimeter or identity management based technologies such as OPM did with their "Shell." Agencies reach this conclusion because existing data centers (a "brownfield" environment) are assumed to be compromised and unsalvageable. The typical response is to stand up a new data center and methodically move workloads and applications from the old data center or brownfield environment to the new greenfield environment or data center once it is operationally ready. This is a legitimate strategy and a process that VMware supports across our customer base.

However, while the overall strategy may be legitimate, it fails to address the persistent security threat to existing cyber infrastructure. There are two main issues with this approach:

- Existing networks or data centers continue to operate while the new environment is being provisioned, which leaves sensitive data vulnerable to continuing attack. It can take months or years to stand up a new greenfield environment. As we've seen, this is what happened with the attack at OPM.
- Without clear cyber security guidelines mandating new software based security strategies that go beyond perimeter-centric security (e.g. Zero Trust or micro segmentation), the new environments are subject to attack as soon as they are operational.

In an era of constrained resources and imminent threat, this approach is insufficient and untimely. Agencies have the ability today to upgrade the security posture of their existing cyber infrastructure to and add Zero Trust software defined solutions that are inherently more cost-effective than new, expensive hardware based solutions. By deploying Zero Trust technologies within our nation's existing networks and data centers, agencies can avoid billions of dollars of additional investment in new greenfield infrastructure when the compelling driver for a greenfield investment is strictly security related.

Summary

VMware is committed to supporting the U.S. Government's efforts to defend our national cyber infrastructure. To be clear, VMware knows that every federal agency, including OPM, is aware of the persistent cyber security threat and is working diligently to address those threats on a daily basis. We applaud the government's efforts and we will continue to encourage them to adopt and deploy the Gold Standard of cyber security across all of their networks.

In our view, all U.S Government Agencies should:

1) For all existing networks, cut the common thread found in every major breach by implementing a Zero Trust security model and reducing attacker/threat mobility within the network.
2) For all new networks, change the way new cyber infrastructure is built and operated by establishing new cyber security standards and metrics that mandate a Zero Trust security model.

VMware sincerely appreciates the opportunity to share our thoughts and suggestions on this very important matter. We applaud the leadership and vision of the Chairmen and Ranking Members in holding this important joint hearing. VMware looks forward to continuing to participate in efforts to improve the security of the federal government. Thank you for the opportunity to testify today.